

UNITED STATES DISTRICT COURT

for the
District of UtahFILED
2024 SEP 4 PM 2:33
CLERK
U.S. DISTRICT COURT

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 4:24-mj-00080 PK

A BLACK ANDROID ONE PLUS WITH A MULTICOLOR
PROTECTIVE CASE

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the _____ District of _____ Utah _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 2252A	Transportation/Receipt/Distribution/Possession of Child Pornography
18 U.S.C. 2242(b)	Coercion/Enticement of Minor

The application is based on these facts:
See attached Affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Christopher Burton

Applicant's signature

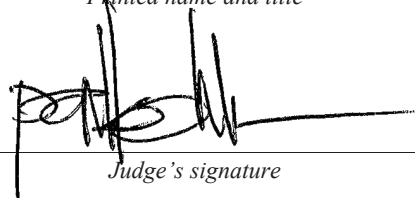
AUSA Christopher Burton

Printed name and title

Sworn to before me and signed in my presence.

Date: September 4, 2024

City and state: St. George, Utah



Judge's signature

United States Magistrate Judge Paul Kohler

Printed name and title

TRINA A. HIGGINS, United States Attorney (#7349)
CHRISTOPHER BURTON, Assistant United States Attorney (NV #12940)
Attorneys for the United States of America
Office of the United States Attorney
20 North Main Street, Suite 208
St. George, Utah 84770
Telephone: (435) 634-4270
Christopher.Burton4@usdoj.gov

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF UTAH

IN THE MATTER OF THE
APPLICATION OF THE UNITED
STATES OF AMERICA FOR A
WARRANT AUTHORIZING THE
SEARCH OF A BLACK ANDROID
ONE PLUS WITH A MULTICOLOR
PROTECTIVE CASE

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR A SEARCH
WARRANT

Case No. 4:24-mj-00080 PK

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

I, Clint Aldred, Detective with the St. George Police Department and Washington County Gang Task Force, being duly sworn, state:

AFFIANT BACKGROUND AND QUALIFICATIONS

1. I have been a peace officer with the St. George Police Department for 4½ years. I completed the Nevada Peace Officer and Standards Training Academy on November 14, 2019. Before my employment with the St. George Police Department, I worked for nine years at the Washington County Sheriff's Office and investigated several

incidents involving drug and gang activity. I have testified before the Grand Jury. I have instructed department training on gang members and their activities. I have also received my waiver as a Utah Peace Officer. I have been a detective investigation fraudulent documents, gang activity, narcotics, and human sex trafficking offenses for approximately three years.

PURPOSE OF AFFIDAVIT

2. I submit this Affidavit in support of an application for a search warrant for a black Android One Plus with a multicolor protective case that was seized from Matthew RADCLIFFE's vehicle on July 23, 2024 (the "Subject Device"), that is currently secured in the evidence room at the St. George Police Department in St. George, Utah.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts in this affidavit are included based on my training and experience, as well as my review of reports written by other law enforcement officers.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. § 2252A(a)(5) (possession of child pornography); 18 U.S.C. § 2252A(a)(2), (distribution/receipt of child pornography); and 18 U.S.C. 2242(b) (coercion/enticement of a minor) have been committed by RADCLIFFE (the "Target Offenses"). There is also probable cause to search the Subject Device described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of the Target Offenses as further described in Attachment B.

SEARCH METHODOLOGY TO BE EMPLOYED

5. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. using hash values to narrow the scope of what may be found. Hash values are used to find previously identified files of images of child pornography and do not capture images that are the result of new production, images embedded in an alternative file format, or images altered, for instance, by a single pixel. Thus, hash value results are under-inclusive, but are still a helpful tool;

f. scanning storage areas;

g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

BACKGROUND REGARDING DIGITAL DEVICES

6. Based upon my training, my experience, and my discussions with other law enforcement agents, I know the following:

a. Users of digital devices increasingly choose to store items in digital form (e.g. pictures, documents) because digital data takes up less physical space, and can be easily organized and searched. Users also choose to store data in their digital devices, such as cell phones, because it is more convenient for them to access data in devices they own, rather than to later spend time searching for it. Keeping things in digital form can be safer because data can be easily copied and stored off site as a failsafe.

b. Users also increasingly store things in digital form because storage continues to become less expensive. Today, 500 gigabyte (GB) hard drives are not uncommon in computers. As a rule of thumb, users with 1 gigabyte of storage space can store the equivalent of 500,000 double spaced pages of text. Thus, each computer can easily contain the equivalent of 250 million pages, that, if printed out, would fill three 35' x 35' x 10' rooms. Similarly, a 500 GB drive could contain 450 full run movies, or 450,000 songs, or two million images. With digital devices, users can store data for years at little or no cost.

c. Storing data in digital form and not deleting it mirrors users' online habits where users have, for years, been encouraged to never delete their E mails. For example, on March 27, 2007, Yahoo! Mail announced free, "unlimited" capacity that gave their users "the freedom to never worry about deleting old messages again." See <[http://ycorpblog.com/2007/03/27/yahoo mail goes to infinity and beyond/](http://ycorpblog.com/2007/03/27/yahoo-mail-goes-to-infinity-and-beyond/)> (accessed April 18, 2012). Similarly, since June 2007, Google, Inc. has promoted free, increasingly larger storage "so you should never have to delete mail."

<[http://gmailblog.blogspot.com/#!/2007/06/welcome to official gmail blog.html](http://gmailblog.blogspot.com/#!/2007/06/welcome-to-official-gmail-blog.html)>; see also <[http://gmailblog.blogspot.com/2007/10/more gmail storage coming for all.html](http://gmailblog.blogspot.com/2007/10/more-gmail-storage-coming-for-all.html)> (accessed April 18, 2012) (promoting its "Infinity+1" plan to constantly give subscribers more storage). Hotmail also has advertised free, "virtually unlimited space," noting that "Hotmail gives you all the space you need." See <<http://www.microsoft.com/windows/windowslive/anotherlookathotmail/storage/>> (accessed April 18, 2012).

d. Digital devices can also store data automatically, without a user's input. For example, network logs may track an employee's actions for company auditing purposes or E mail headers may automatically list the servers which transmitted the E mail. Similarly, a web browser (i.e. an application such as Internet Explorer used to access web pages) can track a user's history of websites visited so users can more easily re access those sites. Browsers also often temporarily cache files from recently accessed web pages to improve the user's experience by reducing that page's loading time. These examples illustrate how the interaction between software and operating systems often

results in data being stored without a user's knowledge. Even if a sophisticated user understands this automatic storage of data, attempts at deleting this data often fail because the data may be automatically stored multiple times and in different locations. Thus, digital evidence may exist despite attempts at deleting it.

e. Digital data is particularly resilient to deletion. First, as noted, data is often automatically stored multiple times in multiple places, where even sophisticated users may not be able to locate. Second, digital data can be recovered years after it has been saved, or viewed B even after such data has been deleted. For example, when a user deletes a file on a computer, the file is sent to the recycle bin, where it can still be retrieved. Even if the file is deleted from the recycle bin, the data does not actually disappear; rather, it remains in “free space” or “slack space” (i.e. in unused space) until it is overwritten by new data. Third, an operating system may also keep deleted data in a “recovery” or “swap” file. Fourth, files from websites are automatically retained in a temporary cache, which are only overwritten as they are replaced with more recently viewed web pages. Thus, the ability to retrieve residues of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer use habits.

DETAILS OF THE INVESTIGATION

7. On July 17, 2024, your Affiant, Detective Clint Aldred, working in the Washington County Focused Operations Group, observed a post on a social media web-based app that, based on my training and experience, was someone asking for information about obtaining Child Sex Abuse Material (CSAM). The post read: “Anyone

purchase a Mega Link? Was it legit or a scam.” Your affiant messaged the account, Mage_Moonlighte, and the person operating the account messaged me back. Mage_Moonlighte asked questions about scams on the internet regarding Mega, a specific cloud-sharing storage commonly used for the storing and distribution of CSAM.

8. Your Affiant then gave an alias account and requested that we move the chat to another social media web-based app. The account JustMe, whom your Affiant suspects is Mathew Radcliffe, messaged me on the new app and indicated that we were messaging on the previous app. He messaged that he had purchased a CSAM link, but the person he purchased it from refused to give him access. He was later granted access to the link and sent the link to me. The link contained 25 files. One file did not work; five files were videos of teens that could be eighteen years old or older, and 19 files depicted minors engaging in sexual activity. One of the files is described as follows:

File Name: 1_5093912770189983886~3

Description: The video depicts a female child, approximately 4 to 6 years old, lying on a bed on her back, completely naked. A completely naked adult male is kneeling to her right near her head. The child engages in oral sex on the male’s erect penis while the male inserts his finger into the child’s vagina. The male then uses a black sex toy shaped like a penis and inserts it into the child’s vagina. This appears to cause the child pain and she winces.

9. On July 19, 2024, JustMe sent me seven CSAM videos through the app.

10. We continued our discussion about what he was into and how he had been chatting and getting files from other people.

9. On 07/23/2024, we were messaging about his weekend and if he found more files or hooked up with anyone. He explained that he did and tied a male up at the male’s request. He said that he had a casita where he did these acts. Your Affiant told

him I was jealous and he messaged, "Well, if you need a place to bring someone," and later said "Oh, would you be willing to share." Your Affiant messaged that Your Affiant was in contact with a boy that was 11. He later asked me to offer him money, and Your Affiant asked how much he was going to pay the child. He told me not to tell the child an amount but to see if that interests him. He said that he would show the minor pornography before engaging in a sexual act. He later described the sex act that he wants to engage in with the 11 year old boy. We made arrangements to meet at a park, but he changed the location to the Fabulous Freddys. Your Affiant told him that Your Affiant would be driving a grey Bronco. The suspect claimed he was in a black SUV.

10. Your Affiant went to the area and told him I was there with the minor. He then said that he would meet us inside to get a drink. Your Affiant continued to wait in the car. He then said that he was inside and that your Affiant and the minor needed to go inside. Your Affiant asked the suspect what he was wearing and the suspect said he was wearing a green shirt, gray shorts, and a trucker's hat. Your Affiant walked in to look for the suspect but as your Affiant walked in, he messaged me saying that your Affiant was alone. Your Affiant called the suspect through the web-based app but he did not answer. The suspect continued to message saying that he did not trust me. Your Affiant then returned to my unmarked vehicle and told the suspect that your Affiant was leaving.

11. Your Affiant saw a male sitting in a silver Kia sedan. Your Affiant recognized the male from when he was walking past my vehicle and looking for an unusually long amount of time at my front passenger window. He also had stayed in the parking lot longer than anyone else.

12. When your Affiant began to leave the parking lot, your Affiant saw the suspect turn on his vehicle. Your Affiant then followed him out and he went southbound on Bluff Street. He then quickly turned right into Specialty Automotive, located at 543 North Bluff Street, and parked near a light pole. Your Affiant attempted to turn around and was facing westbound at the intersection of 500 North and Bluff Street when he saw the suspect facing eastbound at the same intersection. The suspect vehicle had the left turn signal activated and appeared to be in the left turn lane. Your Affiant indicated a right turn onto Bluff Street. However, after your Affiant entered the intersection and began making the right turn, the suspect vehicle instead continued straight, travelling eastbound on 500 North. Your Affiant then turned right on 600 North. When your Affiant arrived at the intersection of 600 North and 600 West, I saw the suspect vehicle travelling north on 600 West, suggesting the vehicle had turned left one block east of Bluff Street. The suspect vehicle was now travelling back to the park where the original meet up was supposed to happen and had essentially driven in a circle.

13. Taskforce detectives conducted a traffic stop on the vehicle at 1300 West Sunset Boulevard. When your Affiant asked the driver, later identified as Matthew Radcliffe, if he had a place to be, he said he was going home. Radcliffe was wearing a green shirt, dark gray/black shorts, and a hat. Your Affiant asked if Radcliffe knew why I was there, and he said no. Your Affiant told Radcliffe that I was the person that he was chatting with and he still claimed he did not know. Your Affiant asked if Radcliffe had ever been questioned about anything like this, and he said he has and that he is a

registered Sex Offender. Your Affiant confirmed that Radcliffe has been previously convicted for possession of Child Sex Abuse Material.

14. Your Affiant then drafted a State warrant to seize and search Radcliffe's cell phone. While drafting the search warrant, your Affiant attempted to again call the suspect through the web-based app. The phone in Radcliffe's vehicle did not ring or vibrate, leading your Affiant to believe that he had deleted the web-based app after exchanging messages with your Affiant at the gas station. The State search warrant was granted, but your Affiant is not relying on that search warrant or the results of the subsequent search to develop probable cause for this search warrant.

15. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called “Face ID.” During the Face ID registration process, the user holds the device in front of his or her face. The device’s camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a

device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is

likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

CONCLUSION

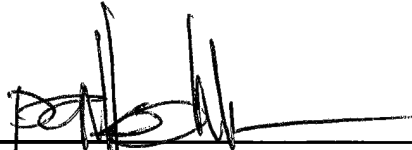
13. Based on the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe that the Subject Device contains evidence of Title 18 U.S.C. § 2252A(a)(5) (Possession of child pornography); 18 U.S.C. § 2252A(a)(1); 18 U.S.C. § 2252A(a)(2) (Distribution/Receipt of child pornography); and 18 U.S.C. § 2242(b) (Coercion/enticement of a minor).

RESPECTFULLY SUBMITTED this ____4th day of August, 2024.



Clint Aldred, Special Agent
St. George Police Department

Subscribed and sworn to before me this 4th day of August, 2024.



JUDGE PAUL KOHLER
United States Magistrate Judge

ATTACHMENT “A”
Property to Be Searched

The Subject Device is described as a black Android One Plus with a multicolor protective case found in Matthew Radcliffe’s possession, and any SIM card contained therein, that is currently secured at the evidence room located at the St. George Police Department located in St. George, Utah.

ATTACHMENT B
LIST OF ITEMS TO BE SEARCHED FOR AND SEIZED

This affidavit is in support of application for a warrant to search a black Android One Plus with a multicolor protective case found in Matthew Radcliffe's possession, and any SIM card contained therein, which is more specifically identified in the body of the application and in Attachment A ("Subject Device"), that can be used to store information and/or connect to the Internet, or which may contain mobile devices, for records and materials that are fruits, evidence, or instrumentalities of violations of 18 U.S.C. § 2252A(a)(5), 18 U.S.C. § 2252A(a)(2), and 18 U.S.C. § 2242(b) (the "Target Offenses"). These records and materials are more specifically identified as:

1. Child pornography, as defined by 18 U.S.C. § 2256(8);
2. Any and all computer software, including programs to run operating systems, applications (like word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs;
3. Any computer-related documentation, which consists of written, recorded, printed or electronically stored material that explains or illustrates how to configure or use computer hardware, software or other related items;
4. Any and all records and materials, in any format and media (including, but not limited to, text messages, SMS messages, picture/video messages, social media communication, envelopes, letters, papers, e-mail, chat logs and electronic messages), pertaining to the Target Offenses;
5. Records and information evidencing occupancy or ownership of the Subject

Device described above, including, but not limited to, sales receipts, registration records, records of payment for Internet access, usernames, passwords, device names, and records of payment for access to newsgroups or other online subscription services;

6. Stored electronic data and related digital storage relating to Global Positioning System (“GPS”) data;

7. Records evidencing the use of the Subject Device’s capability to access the Internet, including: records of Internet Protocol addresses used and records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

8. Images and videos, to include any metadata identifying the date and location of the Subject Device at the time of the photo or video pertaining to the Target Offenses;

9. Evidence of who used, owned, or controlled the Subject Device at the time the things described in this warrant were possessed, accessed, received, created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

10. Evidence of software that would allow others to control the Subject Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software; and evidence of the lack of such malicious software;

11. Evidence of counter-forensic programs (and associated data) that are designed

to eliminate data from the Subject Device;

12. Evidence of the times the Subject Device was used;

13. Passwords, encryption keys, and other access devices that may be necessary

to access the Subject Device.